引用格式：方滨兴. 从“人、财、物”视角出发，提升网络空间的安全态势. 中国科学院院刊, 2022, 37(1): 53-59.
Fang B X. Improving cyberspace security situation from perspective of “Talent, Finance and Infrastructure”. Bulletin of Chinese Academy of Sciences, 2022, 37(1): 53-59. (in Chinese)

从“人、财、物”视角出发，提升网络空间的安全态势

方滨兴

哈尔滨工业大学（深圳） 深圳 518055

摘要 网络安全已经成为保障经济发展、支撑现代科技进步的一个重要环节。随着万物依赖信息技术的应用，提升网络空间的安全态势变得愈发重要。如何采取有力的手段，切实提升网络空间的安全态势，是文章的核心命题。文章提出要从“人、财、物”的角度出发：（1）解决在网络安全人才供应不足的前提下，重点关注从其他信息技术领域平移过来的人才的能力认证问题，旨在向社会供应有细分领域才能的网络安全人才。（2）通过网络安全保险来解决残余风险的转移问题，以便解决在确定的网络安全态势前提下的成本控制问题；同时，通过网络安全保险来提升企业的风险管控水平，降低社会应对网络安全的总成本，树立企业网络安全应对能力的标杆，为企业的社会责任提供有效的应对工具，为网络安全产品提供能力背书。（3）通过“外打内”模式的网络靶场来提升信息技术产品的抗攻击能力，即通过构建符合系统孪生特性的影子系统来承受持续不断的众测，以强化相应系统的安全抗打击能力。通过这3种方式，达到大幅度提升网络安全态势的目标。

关键词 安全态势，人才认定，网络保险，网络靶场，众测

DOI 10.16418/j.issn.1000-3045.20211117006

任何事物的推进，都离不开人、财、物 3 个要素。不同的领域，对“人、财、物”需求的解读是不同的，而在网络安全领域如果能够重点关注“人、财、物”要素，将会显著提升网络空间的安全态势。

1 “人”——强化攻防实践训练，完善网络安全细分领域的人才认证

任何领域都需要人才，这是毋庸置疑的。集成电路等领域对人才的需求具有“静态、聚集”的特点，即人才是聚集在供给侧[①]；而网络安全领域则不同，该领域的人才主要聚集在用户侧，旨在服务于用户运行时的安全问题。政府、教育、信息技术等多个行业对于网络安全具有庞大的用户群需求，导致当前网络安全领域专业人才需求量的庞大缺口；而关注运行时的安全问题，导致行业对网络安全人才的高度依赖性。网络安全领域就好比医疗领域，再好的仪器设备

修改稿收到日期：2021年12月31日

① 集成电路人才缺口仍超 20 万，这些岗位最紧缺 . (2021-10-28)[2021-11-14]. https://www.yicai.com/news/101212081.html.

也仅是辅助手段，最终还是依靠医生来解决“运行时”的问题。

与计算机、通信等领域相比，网络安全教育领域存在的时间不长，人才积累量不够，最近几年的我国在该领域的人才缺口在140万人以上，而每年网络安全相关专业的高校毕业生仅2万余人②。因此，大量的网络安全人才是从信息技术的其他领域横向平移而来。网络安全人才培养的核心问题是，信息技术其他领域人才平移到网络安全领域的核心抓手是什么？网络安全领域如果仅从网络攻防的层面来说，本质上就是对网络应用漏洞的发现利用和遏制对漏洞利用的对抗过程。网络安全领域存在着理论与实践弱关联的特征，即发现漏洞及其利用的过程更多是实践过程，而非仅凭理论分析；同样，发现攻击和对之防御的过程也是以实践为主，而非仅凭理论指导③。这就如同训练搏击运动员，其水平的提高更多是来自于训练与实战。因此，一般性的信息技术领域向网络安全领域平移的抓手应该是攻防实践的训练。

目前来看，攻防实践的最佳支撑点有2个：① 网络靶场，让人们有实践的环境，避免在真实环境中出手而触及法律红线；② 网络攻防演练及网络对抗赛制，激发人们在实践中感受到博弈带来的挑战与成就感。相比西方国家，我国在网络对抗方面处于劣势既是不争的事实，也是国外长期垄断核心信息技术所带来的必然结果。因此，我国在国家之间的网络攻防对抗中极难取得优势。在这种情况下，应大力鼓励网民掌握网络攻防技能、强化攻防实践的训练，以期形成“全民皆兵”“农村包围城市”“打游击战”的战略战术效果。这也是一种通过开辟非对称战场来迂回获取战略优势的模式。

网络安全的人才认定与其他信息技术人才的认定方法不同[1]，原因在于：① 网络安全人才的学历培养人数远远不及岗位的需求人数，无法像其他信息技术人才那样仅靠学历文凭来认证；② 网络安全人才的培养类似于医学生的培养，细分领域专业之间并不具有必然的联系。因此，需要有相应的细分领域的认证模式来应对这一困局。一种创新的网络安全人才认定方法是采取领域适应性的认证模式（图1）：从理论与实践出发，采取自适应的递进式认证模式，旨在通过分层测试来判定被测者可能在某一细分领域具有相应的能力，从而形成面向过程的技能精准评估体系。

网络安全从业者主要是通过继续教育从信息技术领域的其他行业平移过来，如计算机、通信、电子、控制等领域，由此弥补网络安全领域的学历教育人数

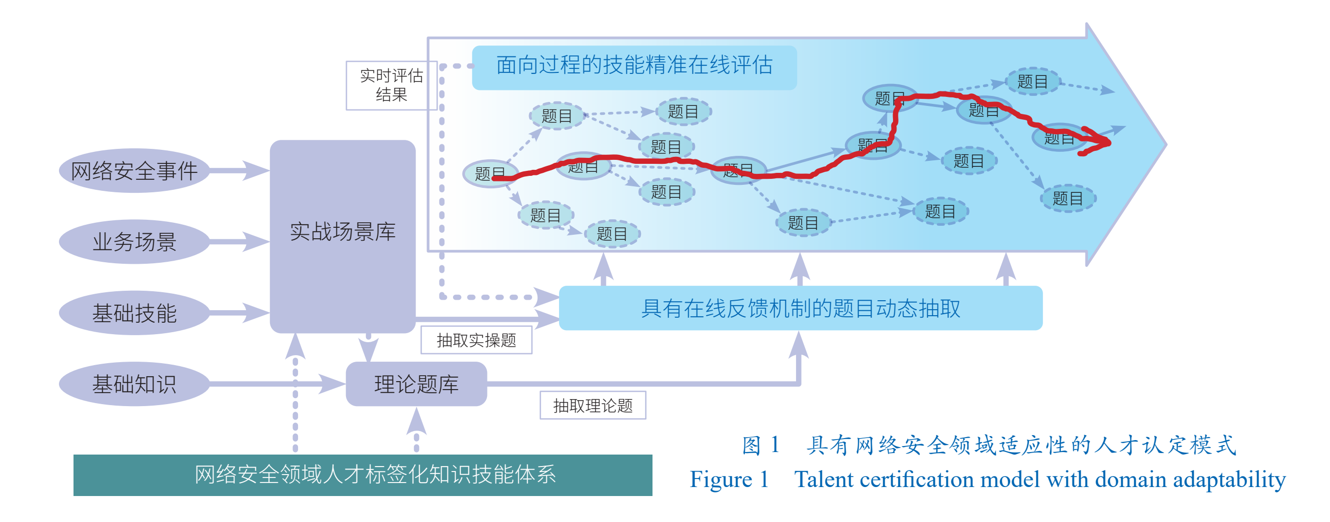


图1　具有网络安全领域适应性的人才认定模式
Figure 1　Talent certification model with domain adaptability

② 工业和信息化部人才交流中心、工业和信息化部网络安全产业发展中心等，《网络安全产业人才发展报告（2021年版）》。
③ 中国网络空间安全人才教育联盟，《网络空间安全工程技术人才培养体系指南》（版本2.0）。

不足的问题。如果企业都拥有经过技能认证的网络安全人才，这势必将从人才的角度来明显提升网络空间的安全态势。

2 “财”——用网络安全保险来提升网络安全生态

网络安全的终极目标是最大限度地减少损失；其中，损失既包含政治层面，也包含经济层面。*从政治层面来看，*网络安全涉及国家安全，关系到经济社会的稳定运行，以及广大人民群众的利益保障；一旦出现问题，其损失往往难以估量。该层面网络安全的目标主要是不惜一切代价来防范攻击，其核心是加大能力建设，如情报发现能力、态势感知能力、体系对抗能力、应急响应能力、容灾备份能力等。*从经济层面来看，*网络安全主要涉及企业的经济损失。该层面网络安全的目标则是要将风险转化成财务指标，要以财务平衡为依据来进行网络安全防范能力的建设。

网络空间是物理空间的延伸，传统的保险并不足以覆盖网络空间带来的风险[2]。*从保险标的角度来看，*传统保险产品大多以有形财产及其相关经济利益和损害赔偿责任为标的；而网络安全的保险标的既包括有形财产，也包括无形财产，如计算机系统、数据、企业声誉等。*从风险环境的角度来看，*传统的保险产品暴露于实体物质环境中，受到的风险多来自意外、自然灾害等；而网络安全保险的风险除了来自实体物质环境之外，还会来自网络空间，如黑客攻击、程序设计错误等。*从赔付对象的角度来看，*传统保险产品的赔付对象主要是第一方损失；而网络安全保险除了第一方损失需要赔付外，还包括第三方损失需要赔付，甚至还会包括危机处理、咨询服务、检测鉴定等费用。

网络安全财务投资具有上限，而残余风险的应对需要依靠网络安全保险。信息系统一旦遭受到攻击，会产生相应的经济损失。因此，被攻击成功的概率与所带来经济损失的乘积就构成了企业网络安全保障的财务指标。也就是说，投资网络安全保障的前提是，降低被攻击成功的概率所带来的经济回报——不应该少于在网络安全保障方面的追加投资。这种追求投入与产出的平衡、而非不惜一切代价的行为，就确定了网络安全财务投资的上限。这就意味着必定存在残余风险需要应对[3]。残余风险的应对需要靠网络安全保险④（图 2）。保险是风险管理的一种财务手段，保险公司通过识别目标风险企业的网络安全风险情况，预测与评估风险，并针对可控的风险来承保企业的网络安全风险，对最终的事故进行经济赔付[4]。因此，保险公司出于对自身盈利的考虑，势必会下力气促进网络安全风险的降低，从而有助于提升网络空间的安全态势。

网络安全保险的核心在于量化网络安全风险的评估[5]，以便用于输出保险方案。其中，量化评估涉及网络安全风险评估和网络安全能力评估；还包括在基于不同风险场景、不同控制措施投入的情况下，对网

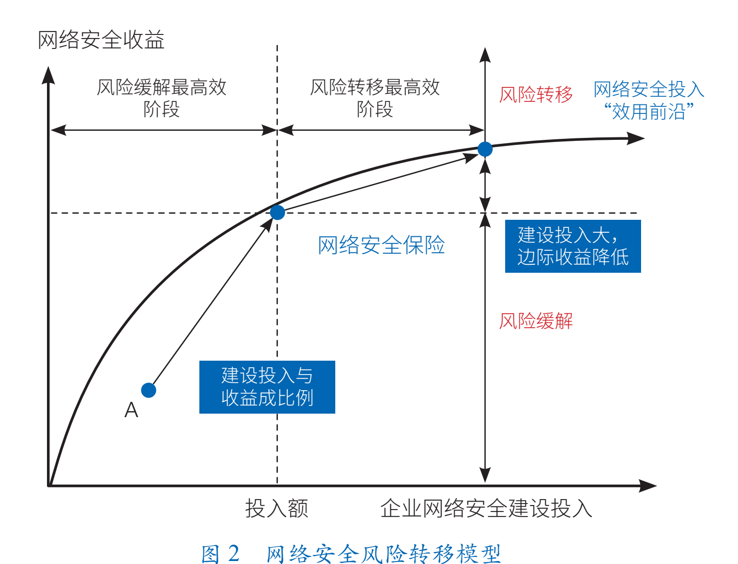


图 2　网络安全风险转移模型
Figure 2　Risk transfer model of cyberspace security

④ Network Security Insurance Policy. [2021-11-14]. https://www.nasinsurance.com/var/documents/P1851NSB-0408.pdf.

络安全成熟度的影响进行定性评估，对网络安全事件发生的概率进行量化评估。研究不同控制措施的投入对网络安全成熟度的影响，从而对网络安全事件发生概率进行量化评估，即可测算出网络安全保险的投资回报率。

网络安全保险之所以能够提升网络安全生态，体现在 5 个方面：① 赋能企业网络安全风险管理。网络安全保险有助于在战略组织层、核心业务层和战术系统层进行风险赋能。② 降低社会总成本，有效降低网络安全事件发生的概率。一方面，可以提高企业的防灾水平——保险公司通过自身的经营活动，可以培养企业的风险意识；另一方面，可以提供专家级的安全服务——保险公司与网络安全企业合作，主动为投保企业提供防灾防损工作，以提高自身的风险收益。③ 树立企业的安全形象。网络安全保险能够提供事前、事中和事后的服务，为客户进一步降低风险。事前，保险公司可识别企业面临的风险类型，针对可控的风险进行承保；事中，通过一定的安全手段及措施对风险进行监控，协助企业降低事故概率；事后，针对安全事故提供及时的安全专家事故支持服务，帮助企业减少事故的损失。由此，保险公司为企业所标称的保险标的，从而通过投保的赔付率来间接反映出投保企业的网络安全防范水平。④ 承担社会责任。国家现已出台了一系列法规政策，强化网络安全保障的要求，但并非所有企业都具有网络安全应对的能力。例如，拥有用户数据的企业可能不具有保护用户数据的能力，但在个人信息保护法的约束下，他们必须承担对用户数据保护的责任。因此，网络安全保险可以成为拥有用户数据的企业来承担其社会责任的一种工具。⑤ 为安全产品的能力背书。对于网络安全产品和服务的提供商而言，网络安全保险可以为他们的产品和服务背书。附赠第三方保险的网络安全产品供应商与服务商，可以通过所附赠的保险额度来展现他们的网络安全应对能力。事实上，网络安全产品供应商与服务商也会为了不断降低保险费用的开销而提升网络安全保障的能力，努力减少网络安全事件的发生。

3 “物”——动态提升信息技术产品与网络安全产品的安全能力

网络安全产品的安全能力是在实践中不断打磨而提升的。传统的网络安全产品的认证模式已经不能适应当前这种网络安全态势快速变化的需要。在当今时代，一个网络安全产品通过认证之后，很有可能会出现一种让该产品无法应对甚至直接攻垮该产品的攻击方式。因此，追求对网络安全产品和可靠、可信信息技术产品的动态、持续的测试愈发重要。

数字孪生[6]是物理世界到数字世界的一个映射。我们也可以构造出相应的系统孪生的产物，这就是为在线运行系统构造出一个相对应的离线“影子系统”，即在同样的系统下所处理的数据并不相同。在这种情况下，可以对“影子系统”进行持续性和安全性测试；一旦发现任何问题，在升级“影子系统”的同时，可以同步升级在线运行系统。为此，构造出能够对“影子系统”持续攻击的环境就变得非常重要。

网络靶场（图 3）是一种由仿真平台所构造出来的攻防环境[7]；以靶标与攻击手是否位于网络靶场内为判定条件，可以组合成“内打内”“内打外”“外打内”和“外打外”4 种攻防模型。① “内打内”攻防模型，指靶标与攻击手都在网络靶场内的情况，主要用于网络安全竞赛（如夺旗赛[8]）、网络安全人员教学训练场景。② “内打外”攻防模型，指攻击手在网络靶场内、靶标在网络靶场外的情况，主要用于组织攻击手在网络靶场内对网络靶场外的真实信息系统目标进行攻击的场景，如护网演练⑤。将攻击手封

⑤ 深圳市公安局启动“护网 2018”网络安全攻防演习 . (2018-12-26)[2021-11-14]. https://baijiahao.baidu.com/s?id=1620915242426467084&wfr=spider&for=pc.

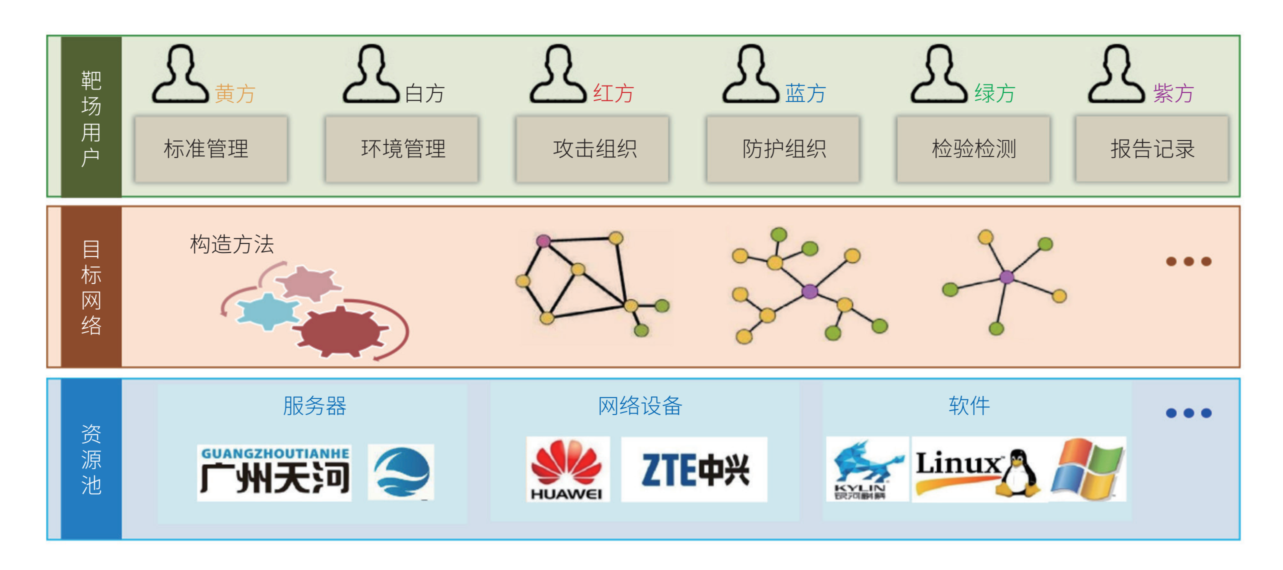


图 3　网络靶场的一般性结构

Figure 3　General structure of cyber range

在网络靶场中的主要目的是防止攻击手在发现漏洞后对真实系统进行不负责任的破坏。③ “外打内”攻防模型，指靶标在网络靶场内、攻击手在网络靶场外，这是一个典型的“众测”模式[9]。将靶标放在网络靶场内用于攻击测试，使得攻击手在网络靶场外可以肆无忌惮地攻击，因为网络靶场内的靶标并没有真实数据，不会出现事实上的损失。通过“悬红”攻击，在让攻击手在获得收益的前提下尽全力检测出靶标的安全缺陷，以便通过不断升级来提升靶标的抗攻击能力。④ “外打外”攻防模型，指靶标与攻击手均在网络靶场外，但攻击手对靶标的攻击则是绕经网络靶场来进行。也就是说，靶标只接受来自网络靶场的连接，所有攻击手只能在监控下通过网络靶场进行攻击。这是因为靶标系统足够大，已经不能迁移到网络靶场之上；而攻击手也足够多或物理位置足够分散，已经不能集中在网络靶场，所以会选择“外打外”的方式来实施“护网”测试演练。

网络靶场的“外打内”模式作为一种众测承载平台，可以成为智慧城市建设中信息基础设施的组成部分，即：对于需要保护的重要信息系统，可以将其“影子系统”以系统孪生的方式部署在网络靶场上，并开放给社会进行众测。如果担心人们缺乏参与众测的动力，还可以通过“悬红”的方式来进行众测，以便检验“影子系统”的安全特性。显然，这将是“双赢”的机会：如果“影子系统”屹立不倒，说明系统孪生所对应的在线运行系统具有强悍的安全防御能力，长期在网络靶场上屹立不倒的系统也会树立起安全口碑；如果“影子系统”被攻垮了，至少也会通过网络靶场的监测了解到问题所在，在提升“影子系统”安全性能的同时也提升了对应在线运行系统的安全防御能力，而这又恰是在网络靶场上部署“影子系统”的核心意图。

在线运行系统尽管事实上也与其“影子系统”同步出现在网络上，但在线运行系统被攻击的概率远比影子系统要小。原因有 3 个：① 法律的保护使得寻常人不敢轻易攻击在线运行系统；② 在线运行系统通常也不会高调出现在网络上让人们所关注；③ 在线运行系统还会配备外围防御系统加以保护，以增加攻击者的难度。而“影子系统”则不同，受到攻击的概率较高：① 大量的网络安全学习者原本就缺少实践环节，尤其是缺少真实的实践场景，所以通常不会放过这种众测的好机会；② “影子系统”也会被高调放到网络

靶场上以吸引人们的关注，至少网络安全企业的竞争者也会从竞争的角度出发来进行各种攻击的尝试；③必要的“悬红”也会吸引那些以“悬红”收入为生存方式的“赏金猎人”积极地参与进来。

可以想象，如果所有的信息技术产品或者网络安全产品都是浸润在网络靶场上经历着众测的千锤百炼，必将会练就一身“本领”，甚至会进入“百毒不侵”的状态。如果人们采用的都是这样的网络产品，以至于没有在网络靶场上放置“影子系统”的产品都不会被人们所采用；在这种情况下，网络安全的安全态势毫无疑问会得到大幅度的提升。

4 结语

网络安全的对抗可以看作是事前、事中、事后 3 个阶段，而网络空间的安全态势取决于在网络安全对抗中是否能够占据优势。从事前角度来看，网络安全的对抗首先是安全设施能力的对抗，当然是防御能力越强，安全态势越好。但是，设备永远是静态的，就算是采用了人工智能的手段，使之会根据态势的变化而具有防御手段动态提升的能力，而其提升方法仍然可以看作是相对静态的。因此，依靠设备来进行网络安全防御所解决的主要是事前的防御。在事中，则更多地要依靠人的能动性，因为只有人才能够在动态博弈中展现出精巧的对抗能力。当然，绝对的安全是不存在的，在事前防御和事中对抗中，总可能出现百密一疏，总是存在着残余风险需要面对的情况。因此，网络安全保险就成为成本控制的救命稻草，需要通过必要的风险转移来解决网络安全防御投入过高的问题。由此，构成了以“人、财、物”为核心来提升网络安全态势的必由之路。

参考文献

1 王惠莅, 王秉政, 杨杰. 网络安全人才标准化研究. 信息安全研究, 2021, 7(6): 520-526.

Wang H L, Wang B Z, Yang J. Research on standardization of cybersecurity workforce. Journal of Information Security Research, 2021, 7(6): 520-526. (in Chinese)

2 王新雷, 王玥. 网络安全保险的策略分析——以网络安全保险的生命流程为研究架构. 情报杂志, 2017, 36(11): 34-40.

Wang X L, Wang Y. Strategic analysis of cyber security risk insurance: Based on the research structure of cyber insurance life process. Journal of Intelligence, 2017, 36(11): 34-40. (in Chinese)

3 李晓勇, 左晓栋. 信息安全的等级保护体系. 信息网络安全, 2004, (1): 18-20.

Li X Y, Zuo X D. The hierarchical protection system of information security. Netinfo Security, 2004, (1): 18-20. (in Chinese)

4 顾建强, 梅姝娥, 仲伟俊. 基于网络安全保险的信息系统安全投资激励机制. 系统工程理论与实践, 2015, 35(4): 1057-1062.

Gu J Q, Mei S E, Zhong W J. Cyber insurance as an incentive for information system security. Systems Engineering-Theory & Practice, 2015, (4): 1057-1062. (in Chinese)

5 贾焰, 方滨兴. 网络安全态势感知. 北京: 电子工业出版社, 2020.

Jia Y, Fang B X. Network Security Situation Awareness. Beijing: Publishing House of Electronics Industry, 2020. (in Chinese)

6 Batty M. Digital Twins. (2018-09-10)[2021-11-14]. https://doi.org/10.1177/2399808318796416.

7 方滨兴, 贾焰, 李爱平, 等. 网络空间靶场技术研究. 信息安全学报, 2016, 1(3): 1-9.

Fang B X, Jia Y, Li A P, et al. Cyber Ranges: State-of-the-art and research challenges. Journal of Cyber Security, 2016, 1(3): 1-9. (in Chinese)

8 Dubey S. An Introduction to Cybersecurity, Capture the Flag Contests, and Basic Security Concepts. (2020-04-17)[2021-11-14]. https://www.siddcodes.com/introduction-to-cybersecurity/.

9 刘小虎, 张玉臣, 张恒巍, 等. 美国国防部网络安全众测的做法、成果及启示. 国防科技, 2019, 40(3): 38-40.

Liu X H, Zhang Y C, Zhang H W, et al. The Practice, achievements and enlightenment of bug bounty programs of the US Department of Defense. National Defense Technology, 2019, 40(3): 38-40. (in Chinese)

Improving Cyberspace Security Situation from Perspective of "Talent, Finance and Infrastructure"

FANG Binxing

(Harbin Institute of Technology (Shenzhen), Shenzhen 518055, China)

Abstract Cyberspace security has been an important part in ensuring economic development and supporting the progress of modern science and technology. As more and more applications are relying on information technology (IT), it becomes very important to improve the security situation of cyberspace. How to take effective measures to practically improve the cyberspace security situation has become the core problem disscussed in this paper. This paper addresses it from the perspectives of "talent, finance and infrastructure". First, on the premise of insufficient supply of cyberspace security talents, this paper proposes to establish the ability certification of talents transferred from other IT fields, in order to provide cyberspace security talents in many subdivided fields. Second, this paper proposes to solve the financial cost control problem under the determined cyberspace security situation through network security insurance, so as to improve the risk control level of enterprises, reduce the cost of social response to cyberspace security, establish the benchmark of response ability, and provide capability endorsement for security products. Third, this paper proposes to improve the anti-attack capability of IT products through the cyber range infrastructure with the "external attack internal" mode, which builds a shadow system to withstand continuous public testing, so as to strengthen the anti-attack capability of the corresponding system. Through the above three ways, the cyberspace security situation can be greatly improved.

Keywords security situation, talent certification, network security insurance, cyber range, public testing



方滨兴 中国工程院院士。哈尔滨工业大学（深圳）计算机科学与技术学院教授、首席学术顾问。信息内容安全技术国家工程实验室主任，中国中文信息学会理事长，中国网络空间安全人才教育论坛理事长，中国网络空间新兴技术安全创新论坛理事长。主要研究领域包括网络靶场、网络空间新技术安全等。E-mail: fangbx@cae.cn

FANG Binxing Academician of Chinese Academy of Engineering. He is the chief academic consultant of College of Computer Science and Technology, Harbin Institute of Technology (Shenzhen), and the director of National Engineering Laboratory for Information Security Technologies. He is also the president of Chinese Information Processing Society of China, the Cyberspace Security Talent Education Forum, and China Cyberspace Security Innovation Alliance on Emerging Technology. His main research interests include cyber range, cyberspace security of emerging technologies, etc. E-mail: fangbx@cae.cn

■责任编辑：张帆

*Corresponding author